CLAIMS

1. System for providing secure service access for a user to at least one service from a service provider,
where the user and the service provider are provided with means for connection to a common computer network, said system comprising:

- one or more validation service units arranged for performing the steps of:
receiving a name in a user certificate from an access server,
controlling the validity of the user certificate,
if the user's certificate is valid, either sending the user's certificate name to an authorization service unit for translation to a user name, and passing the user name returned from the authorization service unit to the access server, or passing the user's certificate name to the access server,
if the user's certificate is not valid, denying the user access to the service;

- one or more authorization service units arranged for performing the steps of:
receiving a user's certificate name from a validation service unit or an access server,
sending the user's certificate name to a database,
receiving user name and profile from the database,
passing the named user identity to the validation service unit or the access server,
receiving a query for access rights from an access server,
querying for subscription info from the database,
receiving subscription info from the database,
determining access rights based on said subscription info,
passing access rights to the access server; and

- one or more authorization role units and adjoining databases arranged for performing the steps of:
receiving a user's certificate from an authorization service unit,
locating the user's name and profile in the database,
sending user's name and profile to the authorization service unit,
receiving a query for subscription info from an authorization service unit,
sending subscription info to the authorization service unit.

2. System according to claim 1,
further comprising at least one access server, arranged for performing the steps of:
receiving a request from the user,
authenticating to user and asking for client authorization,
performing a challenge/response sequence,
requesting a certificate and proof of possession of a private key from the user,

passing the name in the certificate to a validation service unit,
in case of valid user certificate, receiving named user identity from an authorization service unit,
querying an authorization service unit for access rights,
receiving access rights from the authorization service unit,
locating an appropriate service menu,
presenting the service menu to the user, and
transferring information between the user and the service provider.

3. System according to claim 1 or 2,
wherein the access server comprises means for:
supporting HTTPS, or other means for securing communication channels,
authenticating the access server to clients/users, preferably by use of PKI technology,
supporting protocols necessary to communicate with the validation service and the authorization service unit,
supporting one or more protocols for PKI-based client/user authentication,
implementing the functionality needed to display information to the user and to handle user input,
acting as a proxy server between the user and a service.

4. System according to claim 1 or 2,
wherein requesting a certificate and a private key from the user may be performed by using a directory lookup.

5. System according to claim 1 or 2,
wherein the access server is adapted for mediating direct access to the service in a single sign-on manner.

6. System according to claim 1 or 2,
wherein the database storing the user name and profile, is also storing other user related information.

7. System according to claim 3,
wherein the access server, when using other means for securing the communication channel, is establishing a SLL/TLS session with the server authentication only, and running the user authentication protocol on the established secure channel.

8. System according to claim 3,
wherein the user, in case of several alternatives of authentication methods, is presented with the choices, and the access server is establishing a SSL/TLS session with the chosen method of client authentication.

9. System according to claim 5,
wherein the service provider is included in the system and is adapted for accessing and exchanging information with the authorization service unit.

10. System according to one of the claims 1-9,
wherein said validation service units, said authorization service units and said authorization role units are computer-implemented.

11. Use of the system according to claim 1 or 2 for providing authentication, authorization and access to a value-added service such as Video on Demand.

12. Use according to claim 10,
wherein the information is protected by encryption.

13. Method for providing secure service access for a user to at least one service from a service provider,
where the customer and the service provider are provided with means for connection to a common computer network,
said method comprising the steps of:
- by means of one or more validation service units;
receiving a name in a user certificate from an access server,
controlling the validity of the user certificate,
if the user's certificate is valid, either sending the user's certificate name to an authorization service unit for translation to a user name, and passing the user name returned from the authorization service unit to the access server, or passing the user's certificate name to the access server, and
if the user's certificate is not valid, denying the user access to the service;
- by means of one or more authorization service units:
receiving a user's certificate name from a validation service unit or an access server,
sending the user's certificate name to a database,
receiving user name and profile from the database,
passing the named user identity to the validation service unit or the access server,
receiving a query for access rights from an access server,
querying for subscription info from the database,
receiving subscription info from the database,
determining access rights based on said subscription info, and
passing access rights to the access server; and
- by means of one or more authorization role units and adjoining databases:
receiving a user's certificate from an authorization service unit,
locating the user's name and profile in the database,
sending user's name and profile to the authorization service unit,

receiving a query for subscription info from an authorization service unit,
sending subscription info to the authorization service unit.

14. Method according to claim 13,
further comprising the following steps, performed by at least one access server:
receiving a request from the user,
authenticating to user and asking for client authorization,
performing a challenge/response sequence,
requesting a certificate and proof of possession of a private key from the user,
passing the name in the certificate to a validation service unit,
in case of valid user certificate, receiving named user identity from an authorization service unit,
querying an authorization service unit for access rights,
receiving access rights from the authorization service unit,
locating an appropriate service menu,
presenting the service menu to the user, and
transferring information between the user and the service provider.